The ABC of ABC

Korenhof, P.E.I.; Koning, Merel; Alpár, Gergely; Hoepman, J.H.

Published in:
Internet, Law and Politics

Publication date:
2014

Document Version
Early version, also known as pre-print

THE ABC OF ABC: AN ANALYSIS OF ATTRIBUTE-BASED CREDENTIALS IN THE LIGHT OF DATA PROTECTION, PRIVACY AND IDENTITY

Merel Koning
PhD candidate at the Privacy & Identity Lab, based at the ICIS Digital Security, Radboud University Nijmegen

Paulan Korenhof
PhD candidate at the Privacy & Identity Lab, based at Tilburg Institute for Law, Technology and Society (TILT)

Gergely Alpár
PhD candidate at the ICIS Digital Security, Radboud University Nijmegen

Jaap-Henk Hoepman
Associate Professor at the ICIS Digital Security, Radboud University Nijmegen, Scientific Director of the Privacy & Identity Lab

ABSTRACT: Our networked society increasingly needs secure identity systems. The Attribute-based credentials (ABC) technology is designed to be privacy-friendlier than contemporary authentication methods, which often suffer from information overspill. So far, however, some of the wider implications of ABC have not been appropriately discussed, mainly because they lie outside of the research scope of most cryptographers and computer engineers. This paper explores a range of such implications, shows that there are potential risks associated with the wider introduction of ABC in society, and makes the case that legal and societal aspects of ABC be subjected to extended interdisciplinary research.

KEYWORDS: Attribute-based credentials, Authentication, Identification, Data Minimisation, General Data Protection Regulation, Privacy by Design, Data Protection by Design, Socio-Technical Analysis, Legal Analysis.

1. INTRODUCTION

Technology mediates today's data-driven society in which the demands for secure and privacy-friendly digital identity management is growing. Scientist, industry and policy makers have –at least in the past– approached the privacy and security aspects of identity management as being a trade-off between the two. Cryptographic solutions, like attribute-based credentials (ABC), however, enable to build more secure and yet privacy-friendly identity management systems. National governments in the EU are

allocating funds to implement identity management systems and ABC make an interesting candidate. So far, however, there has been little discussion about the wider implications of ABC because they fall outside the normal research field of cryptographers and computer engineers. It has to be admitted that, despite good intentions, ABC implementations nevertheless still introduce a range of societal issues with regard to privacy and identity. Therefore, extended interdisciplinary research on the societal and legal effects of ABC is gaining in relevance.

This paper gives a technical and architectural overview of the ABC concept.

It will continue with an exploration of the reciprocal relationship between the self, identity construction, technology and the architectural decisions within an ABC ecosystem. Furthermore, the paper deals with questions regarding the extent to which an ABC system meets the legal concept of Data Protection by Design and Data Protection by Default.

2. AN OVERVIEW OF ATTRIBUTE-BASED CREDENTIALS

In most computer-related scientific work a digital identity is considered to be a set of characteristics describing certain properties about an individual. This set is dynamic, and depends on the context in which the individual is known. The attribute-based credential technology (Camenisch et al., 2011, Sabouri et al., 2012, Alpár & Jacobs, 2013) implements this model. Personal characteristics, such as age, name, social security number, credit card number as well as more mundane data, like hair colour and favourite dish, are called attributes in this model. Some of these attributes are not directly identifying (e.g. age or hair colour) whereas others are (e.g. name or social security number). [1]

In the conventional identity management model, identity providers are involved in retrieving authentic attributes. After user authentication, the identity provider retrieves and sends personal information about the user to the service provider. This process demands user identification and includes a trusted third party. For example: An individual can use her Facebook account to sign in to a Spotify account.

2.1. The ABC Characteristics

The ABC model stores attributes in a secure container called an attribute-based credential. This credential contains a predetermined set of attributes, whose values are determined by the characteristics of the individual user.

1 The identifying value of certain attributes led to the preference of ABC over the older term anonymous credentials.

Attribute values are reliably verified by an issuer o make sure they match the individual's characteristics. The issuer then secures the attributes in a credential by a digital signature. A municipality, for example, can issue a credential for the attributes of place of birth, residence, date of birth and certain age categories. Once some credentials are issued, the user can disclose a subset of her attributes to a service provider who requires certain information before providing a service. An online video rental store, for example, may need to verify that an individual is over 18 years old before allowing access to an age-restricted movie. Revealing this age category attribute 'I'm older than 18' is done via the mechanism called selective disclosure.

A typical selective disclosure process runs as follows: An individual user selects a service to access. The service provider sends a presentation policy (e.g, Camenisch et al., 2013) to the user asking her to reveal the value for a selection of attributes contained in one or more of her credentials. In order to protect against service providers sending overly broad presentation policies that ask for a non-proportionate selection of attributes, the policies are signed by a scheme authority prior to the selective disclosure process. Service providers can apply for the signature on a certain presentation policy at the scheme authority. They receive this signature after proving the relevance and proportionality of the set of requested attributes. During the selective disclosure process the user verifies this signature before accepting the presentation policy. The user subsequently decides whether she agrees to reveal all the requested attributes. In order to trust the values received, the service provider expects the credentials to be issued by known and trusted issuers. Sometimes, the system allows the user to choose to reveal only a subset of requested attributes. If the user refuses to reveal attributes, the service provider may choose to refuse the user's request, or offer only limited functionality.[2] Once all checks are done the attributes are revealed. Depending on the disclosed attribute values, the service provider can make an access decision.

2.2. The ABC Principles

From a technical point of view ABC must satisfy three requirements: unlinkability, confidentiality and security. The selective disclosure protocol uses zero-knowledge proofs as underlying privacy-enhancing technology (PET). Such zero-knowledge proofs allow a user to convince the service provider about the fact that she owns a credential, signed by the issuer, containing the attribute values disclosed, without showing the full credential itself to the service provider. The proofs achieve unlinkability: Given two proofs of ownership of a particular credential type, it should be impossible to determine (using the proofs alone) whether the same individual produced them or not. Clearly, this is trivial if an identifying attribute is revealed in the selective disclosure. Establishing a secure, encrypted, channel between the user and the service provider typically ensures

2 This is similar to what happens when users refuse to accept cookies or block website scripts.

confidentiality: Only the service provider learns the values of the attributes the user chooses to reveal, and she learns nothing more. For security purposes only the owner of a credential must be able to prove ownership of this credential. Even if several individual requests collude, a user should not be able to convince the verifier that she owns a credential that she originally do not possess. This is partially guaranteed by the fact that issuers sign credentials. This prevents rogue parties to create fake credentials. However, to prevent users to pool or share attributes in credentials, additional mechanisms are necessary. To this end, it is, first of all, assumed that each user has a private key, to which even the user is not privy. Secondly, credentials typically contain an expiry date. To improve the security, some ABC systems store the credentials on a smart card, and let the smart card compute the necessary zero-knowledge proofs.[3]

2.3. The ABC Use Cases

Attribute-based credential systems, especially when implemented on smart cards, can be used both offline and online. An example of an offline use case is the use of a tobacco vending machine. To prevent the sale of tobacco to minors, the vending machine can use ABC technology to verify that the buyer is over 18 (or whatever the appropriate legal limit is). For this to work, users must be able to obtain a credential from the municipality that contains an «over 18» attribute. When buying cigarettes the user inserts her smart card in the vending machine and proves she is over eighteen and from there on continues the purchase transaction.

A typical example of an online use case for ABC is verifying whether a user is subscribed to an online service (such as a digital newspaper or Netflix). These service providers demand strong guarantees that only paying costumers can access the content. With the ABC technology the service provider can issue a credential with an attribute of the type of subscription for every new subscriber. This attribute does not need to contain a membership number (thus, not identifying); access to content can be decided on the type of subscription after the zero-knowledge proof. In this example the service provider is both a credential issuer as well as a relying party towards the attribute.

2.4. The ABC Ecosystems

Scheme authorities play an important role in attribute-based credential schemes. They are responsible for keeping the scheme trustworthy to all stakeholders. Trust is maintained by having a clear policy, describing the roles and responsibilities of all participants in the scheme, and by effectively enforcing this policy. The scheme authority has the power to do so because it can decide

3 For example, the IRMA project (https://www.irmacard.org).

- which issuers are members of the scheme,
- which credentials/attributes a particular issuer can issue,
- which service providers are members of the scheme,
- which credentials/attributes a particular service provider is allowed to access, and,
- which users are issued a card.

These five powers are enforced by the ABC technology. The party that functions as the scheme authority, and the policy that it defines has a major influence on the trust and functionality of the corresponding ABC system. We call a particular instance of an ABC scheme with a certain policy an ecosystem. Several ecosystems can coexist

One possible ecosystem is a national eID system where a government agency is a scheme authority, and whose policy restricts the use of such an eID to government only issuers and service providers. Such a top-down ecosystem has a restricted functionality, but most likely a high level of trust among the service providers while perhaps having a lower level of trust (in terms of privacy) among particular group of users.

A more flexible ecosystem is created by also allowing private sector use of such a government issued eID card. Companies can then serve as issuers and service providers. This hugely increases the number of possible applications of the eID card, but perhaps lowers the overall trust in the system.

Bottom-up, private sector based, approaches are also possible. For example, different companies can decide to issue ABC cards that conform to a certain industry standard that allow arbitrary issuers and service providers to use the platform. In essence in such a setup, no scheme authority is present at all. But small groups of stakeholders may decide to create a scheme authority of their own and use the open platform to create a more closed ABC subsystem. Multiple ABC schemes then coexist on a single card.

3. THE SOCIO-TECHNICAL ASPECTS OF ABC'S

The following section will assess the socio-technical aspects of the techniques discussed above. In today's society authentication is of great importance. Often legal or security rules require individuals to prove certain attributes. Take, for instance, the example of buying tobacco in the previous section. Without an ABC system an individual has to show an ID card to prove the «over 18» attribute, yet these IDs show additional, non-necessary attributes, like date of birth, name, place of birth, gender, etc. Showing additional, non-necessary attributes can be considered an information overspill and gives rise to privacy concerns.

Privacy plays a crucial role for the autonomy of individuals with regard to their identity management (cf. Goffman, 1959). Often, privacy is described in terms of control over personal information. The legal scholar Westin defines privacy as «[...] the

claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others» (Westin, 1966, p. 7). The information scientist Agre defines the right to privacy as «the freedom from unreasonable constraints on the construction of one's own identity» (Agre, 1998, p. 7). A lack of privacy can deprive individuals of choices concerning their self-presentations and the types of social relationships they can establish (Rössler, 2001, p. 112). Privacy breaches can therefore restrict an ndividual in her autonomy to develop her own identity and determine her life plan (Kupfer, 1987, p. 82).

ABC can limit the information overspill. By, for example, only revealing to be over 18 instead of revealing all information on an ID card, ABC systems give technologically dictated privacy safeguards. The selective disclosure of attributes can be an effective means to battle discrimination and aid individuals to control their information.[4] To a certain extent an ABC system improves the autonomy with regard to revealing personal information in different contexts.

Despite these promising facts, ABC form a technology and as such it actively co-shapes the environment in which it is deployed as well as the way individuals relate to one another (cf. Verbeek, 2005). In this capacity ABC systems are interesting to extensively reflect on from a non-technical view. An ABC card is not just an artefact; one cannot simply «use» it. The technology of the ABC card is «a sociotechnical system of use», «a system using combinations of hardware and people (and usually other elements) to accomplish tasks that humans cannot perform unaided by such systems» (Kline, 1985, p. 210-211). The ABC technology is an artefact that reveals whether an individual has or does not have a certain attribute, this is something that without the aid of any artefacts (including ID cards) people are not able to accurately perceive for a majority of attributes. The effects of a new technology cannot be easily predicted until the technology is extensively deployed (Collingridge, 1980). However, due to the potential of ABC in a (future EU obligatory) eID system, we do want to anticipate on the possible impact of ABC on one's autonomy. We will focus on ABC implementations on smart cards.

3.1. Attributes: the 'Haves' and 'Have Nots'

Labelling individuals with certain attributes and others not, could have benefits for both individuals and society in several contexts.[5] The ABC technology provides for an easy means to do so. However ABC technology may not only provide others with

4 E.g. persons who are questioning or experimenting with their gender may not want to share their current legal genderstatus, which may differ from their social identity.

5 See for instance Liagkou, et al. (2014). As the title suggests, this paper is a summary of ABC-4Trust's Greek pilot's setup (results are not included yet). This paper includes a general discussion about the dangers of ABC applications in public opinion polls without thorough analysis

information (individual A has or does not have attribute B) – but it also 'shapes' the information and the manner in which it is experienced. Throughout history people use technology to view the world in a fashion to which they are not capable to do so without the mediation of technology, and in return technology may co-shape the manner in which individuals perceive and interpret themselves and their world (Ihde, 1983, p.22). For instance the use of a thermometer: people cannot feel 'degrees' as such and can only perceive it with the use of this artefact. In return the technology mediates our self-interpretation and interpretation of others. Some people use the thermometer as a decisive factor to regard oneself as ill or verging on ill.

Since the ABC technology sees on identity management, it is important to raise the question how an ABC system would affect the manner in which individuals interpret their identity and that of others. Will this privacy-enhancing technology (PET) lead to a culture in which the individual becomes a 'have' or a 'have not' of certain attributes? ABC systems could potentially be a foundation for the use of overformalized personae because the individual gets access to certain services based on a black-and-white scenario: either one has the attribute or one does not have the attribute. This scenario ignores the –often spacious– gray area between these two extremes, in which many factors play a role in self-interpretation. The types and value options of attributes are therefore of the utmost importance. For instance, with regard to gender Australia recognizes gender X. When an ABC ecosystem only recognizes the attribute values 'female' or 'male', individuals with gender X are limited in their identity-construction in the ABC ecosystem and will be forced to 'fit' into the options offered by the ecosystem. For attribute types and values individuals will be highly dependent on the discretion of the scheme manager and issuers. Thus, the discretionary power of scheme managers and issuers has a far-reaching influence on the autonomy of individuals to shape their identity. An individual cannot 'be' what is not recognised as an attribute in the ecosystem. In return, the attributes allocated to a specific individual can have a reflexive effect with regard to that individual's self-interpretation. For an individual it generally is important to be recognized by others in correspondence with her self-identity. The sociologist Giddens points out that self-identity «has to be routinely created and sustained in the reflexive activities of the individual» (Giddens, 1991, p. 52). This reflexive self-interpretation could be influenced by the allocation of attributes and the continuous confirmation of such attributes within an ABC ecosystem. The result could be that people end up modelling themselves «upon their own artefacts. (...) The creator interprets himself through the created» (Ihde, 1983, p. 74). When thinking of this in the light of potential obligatory use of ABC cards for a wide range of purposes in a wide range of contexts, the question rises whether individuals would start to define themselves and human traits in

and shows that attributes may be important when authenticating for an opinion gathering (polls).

general within the limits of the types and values of attributes recognized within an ABC ecosystem. Even if a wide range of attribute types and values is recognized, the ABC technology still dictates a black-and-white decision; the individual has or does not have a particular attribute, and on this base further decisions are made.

3.2. Function Creep

Technology can be developed for a particular use or purpose. However, oftentimes the technology allows for deployment for other purposes. There is no reason to exclude the applicability of this phenomenon to technology that is initially developed for privacy safeguarding purposes, such as ABC. Technology generally promotes or provokes a specific kind of use (Verbeek, 2005, p. 115), which can stray from the ideas behind the technology.

ABC cards are a technologically dictated reliable source of information and are promoted as 'privacy-friendly' (Camenisch et al., 2010, 2011). An ABC card is much less intrusive than requesting an ID document, e.g. a passport. Businesses and government institutions will –most likely and to a certain extent– encourage its wide range of use, because it is a reliable source of authentic information that they want or need. These entities will be inclined to use ABC to lessen the chance getting accused of privacy-infringements as they use a 'privacy-friendly' technology. As a consequence, more services may ask for an ABC card and attributes. Once there is a nationwide infrastructure supporting ABC[6], and once a large fraction of citizens owns an ABC-like card that is accepted by the majority of businesses and government institutions, the use of this card may become mandatory. Additionally, the cost for asking more information than is strictly necessary is essentially zero. This could lead to the regulation of instances in which a service provider must or may ask for ABC. An individual could then be forced into a position in which she has to identify or authenticate herself in a context in which she previously did not have to do so. ABC can thus have the reverse effect with regard to the initial design idea. This could increase the risk of being profiled; service providers may allow or reject access to certain services based on a small set of attributes. This might lead to discrimination in a new 'jacket'; attribute-based discrimination.

3.3. Authentication Obstructs Obfuscation

Currently there are situations in which an individual does not have to prove her identity in order to get access to a service. For instance, when buying a book online, paying and providing a valid shipping address will generally lead to a successful transaction.

6 E.g. Spirakis & Stamatiou (2013) suggest that the ABC technology will ultimately replace traditional PKI in the context of citizen identity.

However, users are typically required to create an account to finish the transaction. Except for relevant details (like shipping address), people can and do provide fake information for irrelevant account data. Another example is the situation in which an individual wants to get access to a 'personalized' discount card of a grocery shop. Signing up for such a service with an obfuscated identity generally does not hinder the card issuance. In other words, in the current landscape the individual can obfuscate some information without disturbing the service delivery.

ABC cards might influence users in their obfuscation behaviour. Due to the privacy-friendly image of ABC, the urge to obfuscate an identity can decline. However, by using an ABC system, individuals are no longer given a choice to autonomously decide if and what characteristics of their identity they will obfuscate. The consequences of the implementation of ABC systems could be that services like Google and Facebook will have a foolproof way to enforce a real-name policy (Alpár & Jacobs, 2013). Similarly, age-restricted content is truly out of reach for minors. This removes any discretionary decision space for parents (to allow their children access to age restricted content, such as computer games, where the age limit is often set by companies in countries that are different from the age constraint typically enforced in the country of origin), or whistle blowers, researchers or journalists (that would like to use some services without revealing their full name). Over-implementation of an ABC system would diminish individuals their autonomy by depriving them of choices with regard to the manner in which they present themselves or use a pseudonym etc. in several kinds of interactions. Individuals will have to adhere to the norms of the service providers and are left little means to circumvent or negotiate these norms; their behaviour is regulated by technology (cf. Leenes, 2011).

4. ABC'S AND DATA PROTECTION BY DESIGN AND BY DEFAULT

The following section will analyse the compatibility of an ABC system with the concept of Data Protection by Design and Data Protection by Default (DPbD) as proposed in EU Data Protection Regulation. We will focus on the data protection regime as laid down in the European Union.[7] At the time of writing this paper the Regulation[8]

7 Data processing for purposes that fall outside the scope of the jurisdiction of the EU and data processing for criminal law enforcement purposes fall outside the scope of this paper.

8 The Draft version that is used to write this paper is: Report A7-0402/2013 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Date: 21.11.2013. We will refer to this version as: GDPR.

is still in the making. However, despite the fact that the concept of DPbD is not (yet) substantive law, an analysis can be interesting for multiple reasons. Firstly, DPbD can be considered to be the legal obligation to implement privacy-enhancing technologies, such as ABC. Secondly, DPbD relates to the data protection standards as set in article 5(1) sub a of the General Data Protection Regulation (GDPR). These data protection standards date back to the early eighties when they first appeared in international treaties.[9] By testing to these principles, the ABC technology is assessed against the core of the current data protection doctrine. Thirdly, the ABC technology invites the increased usage of pseudonymous data. The GDPR introduces an innovative 'data protection light' regime on pseudonymous data processing. Analysing the legal conditions DPbD could contribute to a better understanding of the privacy enhancement of this technology. Due to the word restrains we will focus on those aspects of DPbD that relate to the sociotechnical aspects.[10]

4.1. The General Obligation of DPbD on the Data Processor

The data protection framework regulates personal data processing. The scope of the term data processing includes any operation that is performed upon personal data, whether or not by automatic means.[11] The term personal data refers to any information relating to a directly or indirectly identified or identifiable natural person.[12] The data protection framework, therefore, does not regulate the design phase of the systems that can process personal data. Knowing this, the EU commission called upon system designers to take responsibility -from a societal and ethical point of view- for the data protection aspects in their systems back in 2007.[13] On top of this appeal and in hope that the data protection standards will permeate into the entire design chain, the EU legislator now introduces DPbD. This new concept lays down a general obligation on the data controller to implement appropriate technical and organizational measures

9 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available on http://www.oecd.org/internet/ieconomy/oecdguidelines ontheprotectionofprivacyandtransborderflowsofpersonaldata.htm Last retrieved on 10 March 2014. EC-Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing C60/48 13 March 1975; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108; Directive 95/46/EC.

10 Further research on the ABC and DPbD is suggested.

11 GDPR article 2 sub b. This includes collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

12 GDPR article 2 sub a.

13 Privacy Enhancing Technologies (PETs) European Commission - MEMO/07/159 02/05/2007.

within the entire life cycle of the technology to ensure data processing to meet the data protection standards.[14]

As explained in the technical overview of ABC, credentials can contain identifying and non-identifying attributes. It follows that when directly identifying attributes are issued or revealed, the issuer or service provider is processing personal data and the Regulation would apply. In case the presentation policy asks for a set of isolation-regarded non-directly identifiable attributes but the combination of the values or the combination with other non-ABC data is identifying, the Regulation also applies. In case the attributes requested in the presentation policy are not directly identifiable and the context allows for certain 'anonymity', the data is anonymous and the Regulation does not apply. In the coming sections we will focus on the processing of personal data. In an ABC ecosystem the issuers and the service providers should be regarded as the data processors: they determine the purposes and the means of the data processing. These entities must ensure the data protection standards and should implement appropriate technical and organizational measures. The substance of DPbD and the data processing standards will be assessed in the coming sections followed by the assessment of the extent to which ABC meet the DPbD obligation.

4.2. The Data Protection Standards

DPbD should be taken into account at the moment of determining the purposes and the means of the data processing as well as at the time of the actual data processing itself. During the entire lifecycle of the data there should be a consistent focus on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. The policy requirements of Data Protection by Default should safeguard that only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data.[15] In the latest version of the GDPR article 23(1) lists the conditions that should be taken into account while implementing the technical and organizational measures. These include: the state of the art current technical knowledge, international best practices and the risks represented by the data processing. The data protection standards are formulated in article 5(1) sub a GDPR. They consist of the general instruction to only process data in a lawful, fair and transparent manner.

14 Recital 61 GDPR.

15 Article 23 GDPR.

The lawful processing standard is embodied by the criterion of legitimate purposes of article 5(1) sub b GDPR. This criterion must be explained in terms of a substantive conception of legality.[16] It does not only refer to the limitative enumeration of legal grounds on which data can be processed in accordance with article 6 of the GDPR, but also to the data controller's duty to determine the purposes and to process personal data in accordance with the law, state-of-the-art techniques and cultural and societal norms.[17] This criterion requires besides a legal assessment, a technology assessment, and hence has a potential propelling effect on the actual implementation of technological innovations. The processing grounds of article 6 GDPR should be obtained prior to –or at the latest at the moment of– the processing of the personal data. At least one of the limitative processing grounds should apply; these grounds vary from consent to a balancing act between the legitimate interests of the data processor and the fundamental rights of the data subject.[18] Consent should be a freely given specific and informed indication of the data subject's wishes.[19]

One would expect an ABC process to be bases on the legitimate ground 'consent' because the user can agree or disagree with the presentation policy.[20] However, as explained in section 2.1 the service provider is entitled to refuse the services in case the data subject does not agree to reveal all attributes that are requested in the presentation policy and the discretionary power of the user to lie about attribute values is limited (section 3.3). One could therefore question whether the ABC systems can process data on basis of consent in all instances; when the alternative is «no service» the freeness of the indication of the data subject's wishes is doubtful.

The purpose limitation principle sets a precondition and demands personal data to be collected for specified, explicit and legitimate purposes (purpose specification) and not to be further processed in a way incompatible with those purposes (use limitation).[21]

16 This broader conception connects the processing grounds to the aspect of foreseeability of article 8(2) European Convention on Human Rights; in the case of interference with the right protected under article 8 there have to be clear, detailed rules specifying the conditions subject to which interferences are legitimate.

17 Article 29 Working Party Purpose Limitation 2013 WP 203.

18 Article 6 a-f GDPR.

19 Recital 25 GDPR.

20 Article 6 sub a GDPR.

21 Use limitation prohibits the further processing of data in case the processing purposes are incompatible with the purposes at the time of the data collection The article 29 Working Party proposed a test in which the relationship of the purposes, the reasonable expectations of the data subject, the nature of the data, impact of the data processing and the safeguards must be weighted in order to determine the compatibility. Article 29 Working Party Purpose Limitation 2013 WP 203, p. 21 and 40.

This principle is of central importance to the whole data protection framework because it fulfils a conditional function for the interpretation of the other fair processing principles, such as adequacy, relevance, proportionality, accuracy, completeness and duration of retention. Like the processing grounds, the purposes need to be specified prior to, and in any event, not later than, the time when the collection of personal data occurs.

The purpose of the use of ABC cards within a particular ecosystem is to a large extent determined by the scheme manager who determines what attribute types are recognized. The issuer decides about the variations in value. These variations determine the possibility for further use too. Take for example the values in the 'gender' attribute from the previous section. The knowledge of gender X can be valuable for further processing for marketing or medical research purposes. The policy aspects influence the further use and purposes. Personal data can only be processed if, and as long as, the purposes cannot be fulfilled by lesser means, such as processing information that does not (directly) involve personal data: pseudonymous data or anonymous data. DPbD also sees on the storage minimization principle: «[P]ersonal data must be kept in a form which permits direct or indirect identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.»[22]

The ABC technology hardcodes the data minimization principle. Once the scheme manager determined what is proportionate and necessary (within the limits of the Regulation) and approves the presentation policies, the data processed for one purpose is minimized to the authorized attribute types coded in the presentation policy. However, as mentioned in the previous section on the socio-technical aspects, function creep is a potentially serious issue for ABC. Since ABC are generally perceived as a privacy-enhancing technology and the system provides strong authentication and a 'good image', societal over-use could be a potential threat to the data processing minimization principle. Besides this, the selective disclosure protocol of ABC empowers the data subject to control the first release of the personal data, however, after that first release the user is just as dependent on the service provider with regard to further use of the data as the subject is in current data processing. Further distribution of the data is not technically regulated by ABC systems and must be regulated by additional policies.

4.3. Pseudonymous Data and Profiling

The GDPR proposes a special 'light' regime on the processing of pseudonymous data.[23] Pseudonymous data should be distinguished from anonymous data, which is information that does not relate to an identified or identifiable natural person. The

22 Article 5(1) sub e GDPR.

23 See Diaz et al. (2008) for an assessment on eID systems and the current legal framework on pseudonymous data.

principles of data protection do not apply to anonymous data. Article 4(2) sub a GDPR defines pseudonymous data as personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution. This light regime particularly affects the legal regime on profiling: forms of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.[24] Profiling based solely on the processing of pseudonymous data is not presumed to be significantly affecting the interests, rights or freedoms of the data subject.[25] However, when profiling –whether based on a single source of pseudonymous data or on the aggregation of pseudonymous data from different sources– permits the controller to attribute pseudonymous data to a specific data subject, the processed data is no longer considered to be pseudonymous.[26]

The use of ABC could have propelling effect on profiling. As described in section 3.2, 3.3. and 4.2 ABC can have a stimulating effect in terms of the quality of data that is revealed (paragraph 3.2 and 3.3) and the quantity of the data processing (3.2 and 4.2). Pseudonymous data is often used for big data and predictive analytics for profiling and targeting purposes. Profiling on the basis of this type of data is not presumed to be significantly affecting the interests, rights or freedoms of the data subject. However, one could question whether profiling with pseudonymous, but verified authentic attributes, will -in the long run- not affect the interests, rights or freedoms of the data subject. With an ABC system the data becomes more valuable and the technology does not regulate the combination or further use of attributes; neither do the policies. The proportionality assessment for the other purposes or further use for which the data might be collected via the ABC card, does not lay in the hands of the scheme manager because this entity only assesses the proportionality with regard to the authentication problem.

24 Article 20 GDPR.

25 Recital 58 a GDPR.

26 Recital 23 GDPR states: The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. Art 10 lid 1. If the data processed by a controller do not permit the controller or processor to directly or indirectly identify a natural person, or consist only of pseudonymous data, the controller shall not process or acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

5. REMAINING ISSUES

When it comes to implications of ABC the sections above are far from comprehensive. In this section we intend to collect further problems that can arise while designing, deploying and operating an ABC system. The technical countermeasures to these potential issues are out of scope in this work because of space limitations and the socio-technical and legal focus of the current research.

A serious security and privacy threat is formed by the user herself. In general, a user is the weakest link of systems security. ABC give the user control and with that more responsibility. For instance, by choosing an easy-to-guess PIN that authorises transactions with service providers, a user risks the protection of her card. Another danger is social engineering that may enable malicious parties to capture the PIN or even the ABC card itself.

In order to have effective control, users should be empowered to check their attribute values. A user-friendly way to do that is by means of a computer or smart phone. This function should be safeguarded by a PIN or biometrics. In spite of the protection a computer or a smart phone is highly untrusted and identity theft via the ABC user panel is not unthinkable. Depending on the ecosystem this attack can become a 'one-stop-shop' for cybercriminals. Moreover, because an ABC card stores a valuable collection of authentic personal data, the business incentive to develop malware (e.g. keylogger, trojan) to acquire these attributes is even bigger.

Malicious activities can also occur on an infrastructural level. Even though an attribute may be anonymous, the 'leaking' of information from another level in the infrastructure, such as an IP address, could make the attribute pseudonymous or even fully identifying; consider for example, the nationality attribute with value 'Australian' in combination with IP address 82.165.102.217. [27]

From an organizational point of view the trustworthiness of the scheme manager is hard to determine. The anonymous aspects of ABC make it even harder to audit the transactions and schemes. Although several revocation techniques have been suggested (Lapon et al., 2011, Hajny & Malina, 2013), the revocation of attributes is still difficult because of the intractability of certain ABC transactions coupled with efficient implementation and proper security (Alpár et al., 2013).

But the utmost difficulty for ABC has to be the mismatch between the idealism behind the technology and the current data-driven society. Personal data is considered the 'new currency' and without an ethical change the data processing practices will most likely not change. Connected to this issue is the nature of humans: people want to share

27 The IP address of the Embassy of Ecuador in London.

data. There are yet to find sufficiently appealing business cases for ABC that compete with the current data processing practices.

6. CONCLUSIONS

Like the legislators in Collingridge's dilemma, we too «face a double-blind prob- lem: the effects of the new technology cannot be easily predicted until the technology is extensively deployed. Yet once deployed they become entrenched and are then difficult to change.» [Collingridge, 1980]. Our attempt was to indicate a set of issues that are likely to arise and –at least– should be given thought before implementation of an ABC ecosystem in society. ABC should be regarded as a socio-technical system that requires co-existence of human and machine. The effects of hard attributes on self-interpretation, the view of others and reflexive self-interpretation should be taken into consideration when assessing this technology. Attribute-based credentials limit the information overspill. But, as described in this paper, this technology does not limit data processing. Due to its privacy-friendly image and verified high quality of data, prompt broad deployment of ABC seems tempting.

However, one could conclude that ABC might have a reverse effect with re- gard to the initial design idea because broad deployment in various contexts may result in stricter authentication than the current practice. The use of ABC cards hinders an individual's strategy in identity obfuscation and the use of fuzzed attributes. ABC diminish the possibility to lie and make informal social agreements. The initial privacy-friendly intent influenced the technical design, but the technical design now influences the 'further' processing purposes. Because of the authenticity of the data and the data protection 'light' regime on pseudonymous data, there is a high probability that information from the ABC will be further used for profiling purposes. In the long run this can affect the rights and freedoms of the data subject. Despite the stimulus data processing for further use might receive from ABC, the technical and policy scheme of ABC only regulates the first use and the proportionality for this initial purpose. Therefore, ABC can be considered 'data protection by design' but they should not by default be considered data protection by default because many aspects are either not covered by the technology or depend on the grace of the scheme manager.

7. BIBLIOGRAPHY

Agre, P.E. (1998). Introduction. In P.E. Agre and M. Rotenberg (Eds.), Technology and privacy: The new landscape (3rd ed., pp. 1-28). Sabon: The MIT Press.

Alpár, G., & Jacobs, B. (2013). Credential design in attribute-based identity management. In Bridging distances in technology and regulation, 3rd TILTing Perspectives Conference (pp. 189-204).

Alpár, G., Hoepman, J. H., & Lueks, W. (2013). An Attack Against Fixed Value Discrete Logarithm Representations. IACR Cryptology ePrint Archive, 2013, 120.

Camenisch, J., Mödersheim, S., Neven, G., Preiss, F. S., & Sommer, D. (2010, June). A card requirements language enabling privacy-preserving access control. In Proceedings of the 15th ACM symposium on Access control models and technologies (pp. 119-128). ACM.

Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K., & Zwingelberg, H. (2011). D2. 1 Architecture for Attribute-based Credential Technologies–Version.

Camenisch, J., Dubovitskaya, M., Lehmann, A., Neven, G., Paquin, C., & Preiss, F. S. (2013). Concepts and Languages for Privacy-Preserving Attribute-Based Authentication. In Policies and Research in Identity Management (pp. 34-52). Springer Berlin Heidelberg.

Diaz, C., Kosta, E., Dekeyser, H., Kohlweiss, M., & Nigusse, G. (2008). Privacy preserving electronic petitions. Identity in the Information Society, 1(1), 203-219.

Giddens, A. (1991). Modernity and self-Identity: Self and society in the late modern age, Standford: Stanford University Press.

Goffman, E. (1959). The Presentation of Self in Everyday Life. London: Penguin Books (used print: 1990).

Hajny, J., & Malina, L. (2013). Unlinkable attribute-based credentials with practical revocation on smart-cards. In Smart Card Research and Advanced Applications (pp. 62-76). Springer Berlin Heidelberg.

Ihde, D. (1983). Existential technics. New York: State University of New York Press.

Leenes, R. (2011). Framing techno-regulation: An exploration of state and non-state regulation by technology. In Legisprudence, 5: 2, p. 143-169.

Liagkou, V., Metakides, G., Pyrgelis, A., Raptopoulos, C., Spirakis, P., & Stamatiou, Y. C. (2014). Privacy Preserving Course Evaluations in Greek Higher Education Institutes: An e-Participation Case Study with the Empowerment of Attribute Based Credentials. In Privacy Technologies and Policy (pp. 140-156). Springer Berlin Heidelberg.

Kline, S. J. (1985). What is technology?. In Bulletin of Science, Technology & Society, 5(3), 215-218.

Kupfer, J. (1987). Privacy, Autonomy, and Self-concept. In American Philosophical Quarterly 24 (1):81 - 89 (1987).

Poller, A. Waldmann, U. Vowé, S., Türpe, S., (2012). Electronic Identity Cards for User Authentication-Promise and Practice. In Journal IEEE Security and Privacy, Volume 10 Issue 1, January 2012 (pp. 46-54).

Rössler, B. (2001). Der Wert des Privaten. Frankfurt am Main: Suhrkamp Verlag (used print: English translation, Cambridge: Polity Press, 2005).

Sabouri, A., Krontiris, I., & Rannenberg, K. (2012). Attribute-Based Credentials for Trust (ABC4Trust). In Trust, Privacy and Security in Digital Business (pp. 218-219). Springer Berlin Heidelberg.

Spirakis, P., & Stamatiou, Y. C. (2013). Attribute Based Credentials Towards Refined Public Consultation Results and Effective eGovernance. In Cyber Security and Privacy (pp. 115-126). Springer Berlin Heidelberg.

Verbeek, P. P. (2005). What things do: Philosophical reflections on technology, agency, and design. University Park, Pennsylvania: Pennsylvania State University Press.

Westin, A. F. (1970). Privacy and freedom. New York: Atheneum.